Efficient Oblivious Proofs Of Correct Exponentiation (Make Corrections)

Markus Jakobsson, Claus Peter Schnorr

Abstract: We study the notion of meta-proofs, which, as the name indicates, are proofs about proofs. We employ the notion of meta-proofs to produce a highly efficient oblivous proof of correct exponentiation. It is minimumknowledge independently of whether the input is valid or not, a property that does not hold for many other protocols (that are zero-knowledge only for valid inputs.) This has direct security implications to multiparty protocols, where the protocols we demonstrate – one interactive and... (Update)